Volume 13, Issue 15   Atari Online News, Etc.   April 15, 2010

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1315   04/15/10

~ Trusted Internet ID Plan ~ People Are Talking!   ~ U.S. Privacy Bill!
~ Jerry Lawson, Game Over ~ Firefox Quicker Updates ~ IE 10 Preview Out!
~ Safari’s "Do Not Track"! ~ Sony, Hotz Settle Suit ~ New Dell Panerai!

~ Harvard Twins Are Stuck! ~ Wii Price Gets $50 Cut? ~ Tablets Hurting PCs!

-* SpyEye Arrests, Little Impact *-
-* Cyberspy vs. Cyberspy, China Wins! *-
-* US Disables Coreflood Botnet, Takes Servers *-

=~=~=~=

->From the Editor’s Keyboard   "Saying it like it is!"

""""""""""""""""""""""""""

The weather is changing for the better lately! While we’re not experiencing "perfect" Spring weather yet, it has been a little bit warmer, the sun is setting later, and my lawn is actually showing more green than brown! Now if we can get the temperatures to rise a little bit more, and I’ll be even more happy.

I haven’t had much time this week to work on editorials, or much of anything else for that matter. It’s become difficult to plan a number of things due to many responsibilities; and usually a few things have to take a back seat. This week, that means some commentary here. So, let’s get to the real stuff this week, and we’ll forego the comments for a bit.

Until next time...

=~=~=~=

```
->In This Week’s Gaming Section  - "Brink" Release Edges Closer!
  """""""""""""""""""""""""""""      Nintendo Cutting Wii Price by $50?
                                     Sony, Hotz Settle PS3 Hacking Suit!
                                     And more!
```

=~=~=~=

->A-ONE’s Game Console Industry News   - The Latest Gaming News!

""""""""""""""""""""""""""""""""""

"Brink" Videogame Release Edges Closer

Bethesda Softworks said Monday that its new "Brink" videogame set in an Earth flooded due to climate change will be released on May 10, a week ahead of schedule.

"Production wrapped on Brink earlier than we planned and we didn’t see any reason to keep gamers from getting their hands on this highly anticipated game as soon as it was ready," said Bethesda marketing vice president Pete Hines.

"It’s apparent from the tremendous reaction so far that people are eager to jump online and play, and if we can make that happen earlier - we’re going to."

Bethesda, the US publisher behind a blockbuster "Fallout" franchise that combines upbeat 1950s pop culture with the aftermath of nuclear war, had Splash Damage studio craft the "Brink" first-person shooter videogame.

US consumer electronics chain Best Buy was enticing players to pre-order "Brink" by promising to add software that will let them customize a character in the "Fallout" theme.

"Brink" takes place "in the near future" in an enormous floating city crammed with ten times more people than it was designed to support.

Battles play out between the Ark’s governing powers and rebels out to seize control along with precious resources such as food and water.

"Brink" videogames for play on Xbox 360 or PlayStation 3 consoles will be priced at $60, while a version tailored to personal computers powered by Windows software will cost 10 dollars less.

"Brink" will be released in Europe three days after its North America debut on May 10.

Nintendo Cutting Wii Price by $50

To help push dusty Nintendo Wii’s off the shelves, Nintendo is reportedly dropping the price of its console to $150, from $199.

Citing an unnamed source, Engadget reported on Monday that the new price will take effect on May 15.

A spokesman for Nintendo said, "Nintendo does not comment on speculation or rumor." Engadget pointed to a March interview between Nintendo America president Reggie Fils-Aime and Gamasutra, in which Fils-Aime discussed re-pricing the console.

"The Wii has a long life in front of it," Fils-Aime said. "We’re still sitting at $199. There are a variety of marketing tools at our disposal."

In late March, Fils-Aime told CNN that 3D will not be the star feature in the Nintendo’s next-generation console, which is expected soon as the Wii turns five years old this year.

The Nintendo Wii, once the hottest console in the U.S., has seen its popularity fizzle somewhat within the last year. In February, Wedbush analyst Michael Pachter said Wii sales had dropped 31.5 percent in January (usually a big month for console purchases) as consumers opted for newer motion-control technologies like the Kinect for Xbox 360. However the Wii still leads the current console market with 34.5 million units sold in the

U.S., followed by Microsoft’s Xbox 360 with 25.8 million, and Sony’s PlayStation 3 at 15.7 million, NPD reports.

After delays due to the Japan earthquake and tsunamis, Nintendo’s Pokemon franchise on Wednesday will launch Pokemon Global Link, a Web site where "Pokemon Black" and "Pokemon White" users can access post-game worlds, Dream World and Global Battle Union. The new feature also lets users save their progress online.

Sony, Hotz Settle PS3 Hacking Suit; Hotz Vows Boycott

Sony and George "Geohot" Hotz said Monday that the two sides have mutually agreed to settle their suit, which includes Hotz agreeing to a permanent injunction against posting information that Sony has wanted removed.

The settlement was reached on March 31, the two sides said in a statement.

Sony is glad to put this litigation behind us," said Riley Russell, general counsel for Sony Computer Electronics America (SCEA), in a statement. "Our motivation for bringing this litigation was to protect our intellectual property and our consumers. We believe this settlement and the permanent injunction achieve this goal."

"It was never my intention to cause any users trouble or to make piracy easier," said Hotz, "I’m happy to have the litigation behind me."

On his Web page, however, Hotz claimed that he would never purchase a Sony product again. "As of 4/11/11, I am joining the Sony boycott," he wrote on his blog. "I will never purchase another Sony product. I encourage you to do the same. And if you bought something Sony recently, return it."

Hotz also claimed that "there is much more to come on this blog". On Sunday, Hotz posted an image with the caption: "I am in ur blogz/censoring ur speeches".

In January, lawyers representing Hotz argued that he hacked the PS3 to add back a feature that Sony had removed. Hotz, the lawyers claimed, "re-enabled" OtherOS functionality, or the ability to dual-boot the PlayStation 3 using some other OS, such as Linux.

SCEA filed suit against George Hotz (AKA "geohot") as well as "Bushing," Hector Martin Cantero, Sven Peter, and others alleged to be part of the FAIL0VERFLOW group of hackers that contributed to the release of the PlayStation 3’s root key. SCEA charged Hotz and the others with violations of the Digital Millennium Copyright Act, the Computer Fraud and Abuse Act, plus breaches of California copyright law, breach of contract, and other violations.

SCEA also asked the court for a temporary restraining order preventing the plaintiffs from posting any code, including the so-called Elliptic Curve Digital Signature Algorithm keys, encryption keys, dePKG firmware decrypter, or other tools - the injunction Hotz apparently agreed to.

The case then took a turn for the odd, with Sony claiming that Hotz fled the country with several key components of hard drives that contained the code. For his part, Hotz claimed that he was on "spring break".

Hotz had attempted to claim that the California court had no jurisdiction in the case, as Hotz was a resident of New Jersey. That complaint is still in front of the court.

The Sony statement also made clear that Hotz was not part of the recent attacks against Sony by "Anonymous". The group said that it plans to protest and boycott Sony stores on April 16, an action Hotz plans to join.

Jerry Lawson, Inventor of Modern Game Console, Dies at 70

Gerald "Jerry" Lawson, creator of the first cartridge-based videogame console, died Saturday morning in a Mountain View, California, hospital, Wired.com has learned. Lawson was 70.

As an engineer at Fairchild Semiconductor, Lawson designed the electronics of the Fairchild Video Entertainment System, later renamed the Channel F, in 1976.

Predating the release of Atari s Video Computer System by a year, the Channel F was the first videogame machine that used interchangeable game cartridges, which Fairchild sold separately. Previous game machines like Atari s Pong and the Magnavox Odyssey had all their games built into the hardware. Lawson s pioneering design set the standard for the game consoles of today.

"Jerry was an amazing personality," said family friend David Erhart, who broke the news of Lawson s death Monday on the Digital Press website. "He created part of the videogame industry history in Silicon Valley and it was always a pleasure to hear his stories about back in the day."

Much of Lawson s background is discussed in a wide-ranging interview he gave Vintage Computing and Gaming in 2009.

A lifelong engineer and tinkerer, Lawson was born in 1940 and grew up in a federal housing project in Queens, New York. As a kid, he operated a ham radio; as a teenager he earned money by repairing his neighbors television sets.

In the 1970s, living and working in Silicon Valley, he joined the Homebrew Computer Club, a group of early hackers that included Apple co-founders Steve Jobs and Steve Wozniak.

Lawson s contributions to videogames began with Demolition Derby, a coin-operated arcade machine that he created in his garage while working at Fairchild.

"Fairchild found out about it - in fact, it was a big controversy that I had done that. And then, very quietly, they asked me if I wanted to do it for them," Lawson said in the Vintage Computing interview.

Although similar machines were in development at Atari and RCA at the time, the console Lawson s team built for Fairchild was the first cartridge-based gaming system that came to market. Although it seems simple now, making the technology work wasn t easy.

"There was a mechanism that allowed you to put the cartridges in without destroying the semiconductors". We were afraid - we didn t have statistics on multiple insertion and what it would do, and how we would do it, because it wasn t done. I mean, think about it: Nobody had the capability of plugging in memory devices in mass quantity like in a consumer product. Nobody."

Only 26 cartridges were ever released for Channel F, all simple games like Blackjack, Space War and Bowling. When Atari released its cartridge-based system, Channel F was quickly rendered obsolete. Years later, Lawson started his own company, Videosoft, to produce Atari 2600 cartridges, but only released one, a technician s tool called Color Bar Generator.

Last month, the International Game Developers Association honored Lawson s pioneering efforts at Game Developers Conference in San Francisco. His workbench had more tools than most people would even know what to do with.

"The whole reason I did games was because people said, You can t do it, " he told the San Jose Mercury News last month. "I m one of the guys, if you tell me I can t do something, I ll turn around and do it."

In later years, Lawson had suffered the severe effects of diabetes. He lost sight in one eye and lost one of his legs to the disease, leaving him confined to a wheelchair. On Wednesday, not feeling well, he was admitted into El Camino Hospital Mountain View.

"He continued building devices to control telescopes, lasers, tools, etc. up until the day he went to the hospital," said friend Erhart. "His workbench had more tools than most people would even know what to do with. He taught me quite a bit and I ll miss him sorely."

At 6:15 a.m. Saturday, Lawson died after apparently suffering a heart attack. He is survived by his wife, son and daughter. The family is planning a memorial service in mid-May.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

John McCain, John Kerry Introduce Contentious U.S. Privacy Bill

Senators John Kerry and John McCain introduced a tough new privacy bill on Tuesday that would require companies to notifyconsumers in clear language when their data is being collected and oblige them to keep that information safe from hackers.

There are increasing concerns about the amount of information companies collect about consumers and how they safeguard it. Millions of people face a heightened risk of email swindles after a massive security breach suffered by Epsilon, an online marketing firm with hundreds of firms among its clients.

The bill would apply to hundreds of companies from search engine giant Google Inc to telephone companies such as AT&T Inc to cable companies such as Verizon Communications Inc and Comcast Corp.

The bill, if it becomes law, would require companies to tell consumers why data was being collected, whom it would be shared with and how it would be safeguarded.

Companies collecting data must also allow consumers to opt out of some data collection and they must agree, or opt in, to the collection of sensitive data like medical conditions.

The bill would also press businesses to collect only the information needed for any particular transaction.

Kerry, a Democrat from Massachusetts, said the measure had support from some big technology companies.

"These companies agree with us that it doesn’t just make good business sense to protect their customer; they know it’s the right thing to do," he told a news conference.

McCain, an Arizona Republican, noted many websites - like most search engines - are free precisely because they are supported by advertising.

"Our bill seeks to respect the ability of businesses to advertise, while also protecting consumers’ personal information," said McCain.

The administration said it liked aspects of the legislation and was carefully reviewing other elements.

Hewlett-Packard Co, Microsoft Corp, eBay Inc and Intel Corp all support the bill.

"We have long advocated for comprehensive federal privacy legislation," they said in a joint statement. "The complexity of existing privacy regulations makes it difficult for many businesses to comply with the law."

The bill seeks to protect data that is unique to a person, such as their name, physical address, email address, telephone number, Social Security number and credit card numbers.

Enforcing the bill would fall to the Federal Trade Commission and to state attorneys general, with the FTC taking the lead.

Attorneys general would be limited to seeking a $3 million penalty for violating security and transparency rules. The FTC might levy civil penalties of $16,000 per violation per day.

California lawmakers are considering a "do not track" bill, which the Kerry/McCain measure would preempt.

This was not a concern, said a congressional staffer who argued it was impossible to have state-by-state regulation of data collection.

"At the end of the day, this is interstate commerce," the staffer said.

The bill was a disappointment to the Direct Marketing Association, which argued it risked damaging the Internet at a time when it was a vibrant spot in the U.S. economy. In 2010, companies spent more than $25.4 billion on digital advertising, which generated $503.6 billion in sales, DMA said.

"DMA is wary of any legislation that upsets the information economy without a showing of actual harm to consumers," said Linda Woolley, a DMA executive vice president.

It was also a disappointment to a coalition of consumer groups and privacy advocates, which welcomed the bill but called for it to be "significantly strengthened."

"I don’t think this is going to affect online marketing at all," said Jeff Chester, director of the Center for Digital Democracy privacy group.

John Simpson, of Consumer Watchdog, agreed.

"We cannot support it today," he said.

White House Releases Trusted Internet ID Plan

The U.S. government will coordinate private-sector efforts to create trusted identification systems for the Internet, with the goal of giving consumers and businesses multiple options for authenticating identity online, according to a plan released by President Barack Obama’s administration.

The National Institute of Standards and Technology (NIST) will work with private companies to drive development and adoption of trusted ID technologies, White House officials said. The National Strategy for Trusted Identities in Cyberspace (NSTIC), released by the Department of Commerce on Friday, aims to protect the privacy and security of Internet users by encouraging a broad online authentication market in the U.S.

"The fact is that the old password and username combination we often use to verify people is no longer good enough," Commerce Secretary Gary Locke said at an NSTIC release event hosted by the U.S. Chamber of Commerce. "It leaves too many consumers, government agencies and businesses vulnerable to ID and data theft."

Because of online fraud, many people don’t trust the Internet, Locke added. "It will not reach its full potential - commercial or otherwise - until users and consumers feel more secure than they do today when they go online," he said.

About 8.1 million U.S. residents were victims of ID theft in 2010, Locke said. The cost to business is high: a company with 500 employees spends about US$110,000 a year managing employee IDs, according to the Department of Commerce.

The trusted ID technologies described in NSTIC would allow online users to dump passwords in favor of credentials that can be used on multiple websites. The Obama administration hopes that multiple trusted ID technologies will emerge, officials said.

Consumer participation in trusted ID technologies will be voluntary, they added.

NIST will host three workshops starting in June to focus on problems with development and adoption of online ID authentication technologies, Obama administration officials said. Businesses, consumer groups, privacy advocates and other interested members of the public will be invited, they said.

The plan aims for several trusted ID pilot projects to be launched in 2012, and the administration hopes to see a robust trusted ID market in the U.S. in three to five years, officials said.

The White House released a draft version of NSTIC in June. The new version more explicitly emphasizes that the private sector will drive forward the trusted ID market, with government playing a coordinating role, administration officials said.

After the draft release, some critics raised privacy concerns about NSTIC, suggesting it is the administration’s effort to create a national ID. The emphasis on private sector leadership should debunk that argument, Locke said.

"Other countries have chosen to rely on government-led initiatives to essentially create national ID cards," he said. "We don’t think that’s a good model, despite what you might have read on blogs frequented by the conspiracy theory set. Having a single issuer of identities creates unacceptable privacy and civil liberties issues. We also want to spur innovation, not limit it."

Privacy advocate Susan Landau, a fellow at Harvard University, praised the new version of NSTIC, saying it will allow Internet users to remain anonymous for many online transactions. The plan calls for online businesses to collect the minimal amount of information necessary from credential providers in order to process the transaction, administration officials said.

"NSTIC certainly sets out the right vision here," added Leslie Harris, president and CEO of the Center for Democracy and Technology (CDT), a privacy advocacy group. "It gives consumers more control and more choice about their online identities. It makes it clear that it’s voluntary."

Representatives of several vendors, including Google and Paypal, praised the effort. Several vendors demonstrated trusted ID technologies at the event, with Northrop Grumman, Microsoft and other partners demonstrating a cloud-based credential system for mobile devices.

US Disables ’Coreflood’ Botnet, Seizes Servers

US authorities on Wednesday announced the disabling of a vast network of virus-infected computers used by cyber criminals to steal millions of dollars.

The "Coreflood" botnet is believed to have operated for nearly a decade and to have infected more than two million computers around the world, the Justice Department and FBI said in a joint statement.

They said charges of wire fraud, bank fraud and illegal interception of electronic communications had been filed against 13 suspects identified in court papers only as John Doe 1, John Doe 2, etc.

The complaint said they were all "foreign nationals" but provided no further information about their identities or nationalities.

Five "command and control" computer servers and 29 Internet domain names were seized as part of the operation, described as the "most complete and comprehensive enforcement action ever taken by US authorities to disable an international botnet."

A botnet is a network of malware-infected computers that can be controlled remotely from other computers.

Coreflood, which exploited a vulnerability in computers running Microsoft’s Windows operating systems, was used to steal usernames, passwords and other private personal and financial information, US officials said.

As of February 2010, some 2.33 million computers were part of the Coreflood botnet, including 1.85 million in the United States, according to the complaint filed with the US District Court for the District of Connecticut.

"Infected computers in the Coreflood botnet automatically recorded the keystrokes and Internet communications of unsuspecting users, including online banking credentials and passwords," the complaint said.

"The defendants and their co-conspirators used the stolen data, including online banking credentials and passwords, to direct fraudulent wire transfers from the bank accounts of their victims," it added.

The complaint said the full extent of the financial loss is not known but it provided details on a number of victims.

They included a real estate company in Michigan hit for $115,771 in fraudulent wire transfers, an investment company in North Carolina taken for $151,201 and a defense contractor in Tennessee which lost $241,866.

Dave Marcus, research and communications director at McAfee Labs, said the cyber criminals behind Coreflood were apparently able to "turn the botnet into a money making machine."

"It is hard to estimate the actual loot, but the criminals likely made tens of millions of dollars, based on the estimates in the complaint filed by the Department of Justice," Marcus said. "It is not outside of the realm of possibility that they netted more than $100 million."

US attorney David Fein said the seizure of the Coreflood servers and the Internet domain names "is expected to prevent criminals from using Coreflood or computers infected by Coreflood for their nefarious purposes."

"These actions to mitigate the threat posed by the Coreflood botnet are the first of their kind in the United States and reflect our commitment to being creative and proactive in making the Internet more secure," added Shawn Henry of the FBI’s Criminal, Cyber, Response and Services Branch.

In July of last year, US, Spanish and Slovenian law enforcement authorities announced the arrest of the suspected creator of the "Mariposa Botnet," which may have infected as many as eight million to 12 million computers around the world.

In Cyberspy vs. Cyberspy, China Has The Edge

As America and China grow more economically and financially intertwined, the two nations have also stepped up spying on each other. Today, most of that is done electronically, with computers rather than listening devices in chandeliers or human moles in tuxedos.

And at the moment, many experts believe China may have gained the upper hand.

Though it is difficult to ascertain the true extent of America’s own capabilities and activities in this arena, a series of secret diplomatic cables as well as interviews with experts suggest that when it comes to cyber-espionage, China has leaped ahead of the United States.

According to U.S. investigators, China has stolen terabytes of sensitive data - from usernames and passwords for State Department computers to designs for multi-billion dollar weapons systems. And Chinese hackers show no signs of letting up. "The attacks coming out of China are not only continuing, they are accelerating," says Alan Paller, director of research at information-security training group SANS Institute in Washington, DC.

Secret U.S. State Department cables, obtained by WikiLeaks and made available to Reuters by a third party, trace systems breaches - colorfully code-named "Byzantine Hades" by U.S. investigators - to the Chinese military. An April 2009 cable even pinpoints the attacks to a specific unit of China’s People’s Liberation Army.

Privately, U.S. officials have long suspected that the Chinese government and in particular the military was behind the cyber-attacks. What was never disclosed publicly, until now, was evidence.

U.S. efforts to halt Byzantine Hades hacks are ongoing, according to four sources familiar with investigations. In the April 2009 cable, officials in the State Department’s Cyber Threat Analysis Division noted that several Chinese-registered Web sites were "involved in Byzantine Hades intrusion activity in 2006."

The sites were registered in the city of Chengdu, the capital of Sichuan Province in central China, according to the cable. A person named Chen Xingpeng set up the sites using the "precise" postal code in Chengdu used by the People’s Liberation Army Chengdu Province First Technical Reconnaissance Bureau (TRB), an electronic espionage unit of the Chinese military. "Much of the intrusion activity traced to Chengdu is similar in tactics, techniques and procedures to (Byzantine Hades) activity attributed to other" electronic spying units of the People’s Liberation Army, the cable says.

Reconnaissance bureaus are part of the People’s Liberation Army’s Third Department, which oversees China’s electronic eavesdropping, according to an October 2009 report by the U.S.-China Economic and Security Commission, a panel created by Congress to monitor potential national security issues related to U.S- China relations. Staffed with linguists and technicians, the Third Department monitors communications systems in China and abroad. At least six Technical Reconnaissance Bureaus, including the Chengdu unit, "are likely focused on defense or exploitation of foreign networks," the commission report states.

The precise relationship with the Chinese Army of suspected hacker Chen Xingpeng could not be immediately determined by Reuters. A spokesman for the Chinese embassy in Washington did not respond to multiple requests for comment. The U.S. State Department declined to comment.

But the leaked cables and other U.S. government reports underscore how Chinese and other state-sponsored and private hackers have overwhelmed U.S. government computer networks. In the last five years, cyber-intrusions reported to the U.S. Computer Emergency Response Team, a unit of the Department of Homeland Security, have increased more than 650 percent, from 5,503 incidents in fiscal 2006 to 41,776 four years later, according to a March 16 report by the Government Accountability Office.

The official figures don’t account for intrusions into commercial computer networks, which are part of an expanding cyber-espionage campaign attributed to China, according to current and former U.S. national security officials and computer-security experts.

In the last two years, dozens of U.S. companies in the technology, oil and gas and financial sectors have disclosed that their computer systems have been infiltrated.

In January 2010, Internet search giant Google announced it was the target of a sophisticated cyber-attack using malicious code dubbed "Aurora," which compromised the Gmail accounts of human rights activists and succeeded in accessing Google source code repositories.

The company, and subsequent public reports, blamed the attack on the Chinese government.

The Google attack "was certainly an escalation of Chinese network operations against the U.S.," says Joel Brenner, former counterintelligence chief for the Office of the Director of National Intelligence. "Thousands" of U.S. companies were targeted in the Aurora attacks, Brenner says - far more than the estimated 34 companies publicly identified as targets so far - a scale which Brenner says demonstrates China’s "heavy-handed use of state espionage against economic targets."

Many firms whose business revolves around intellectual property - tech firms, defense group companies, even Formula One teams - complain that their systems are now under constant attack to extract proprietary information. Several have told Reuters they believe the attacks come from China.

Some security officials say firms doing business directly with Chinese state-linked companies - or which enter fields in which they compete directly - find themselves suffering a wall of hacking attempts almost immediately.

The full scope of commercial computer intrusions is unknown. A study released by computer-security firm McAfee and government consulting company SAIC on March 28 shows that more than half of some 1,000 companies in the United States, Britain and other countries decided not to investigate a computer-security breach because of the cost. One in 10 companies will only report a security breach when legally obliged to do so, according to the study.

"Simply put, corporations cannot afford negative publicity (about computer security breaches)," says Tom Kellermann, vice president of security awareness at Core Security Technologies and a contributor to the study.

What is known is the extent to which Chinese hackers use "spear-phishing" as their preferred tactic to get inside otherwise forbidden networks. Compromised email accounts are the easiest way to launch spear-phish because the hackers can send the messages to entire contact lists.

The tactic is so prevalent, and so successful, that "we have given up on the idea we can keep our networks pristine," says Stewart Baker, a former senior cyber-security official at the U.S. Department of Homeland Security and National Security Agency. It’s safer, government and private experts say, to assume the worst - that any network is vulnerable.

Two former national security officials involved in cyber-investigations told Reuters that Chinese intelligence and military units, and affiliated private hacker groups, actively engage in "target development" for spear-phish attacks by combing the Internet for details about U.S. government and commercial employees’ job descriptions, networks of associates, and even the way they sign their emails - such as U.S. military personnel’s use of "V/R," which stands for "Very Respectfully" or "Virtual Regards."

The spear-phish are "the dominant attack vector. They work. They’re getting better. It’s just hard to stop," says Gregory J. Rattray, a partner at cyber-security consulting firm Delta Risk and a former director for cyber-security on the National Security Council.

Spear-phish are used in most Byzantine Hades intrusions, according to a review of State Department cables by Reuters. But Byzantine Hades is itself categorized into at least three specific parts known as "Byzantine Anchor," "Byzantine Candor," and "Byzantine Foothold." A source close to the matter says the sub-codenames refer to intrusions which use common tactics and malicious code to extract data.

A State Department cable made public by WikiLeaks last December highlights the severity of the spear-phish problem. "Since 2002, (U.S. government) organizations have been targeted with social-engineering online attacks" which succeeded in "gaining access to hundreds of (U.S. government) and cleared defense contractor systems," the cable said. The emails were aimed at the U.S. Army, the Departments of Defense, State and Energy, other government entities and commercial companies.

Once inside the computer networks, the hackers install keystroke-logging software and "command-and-control" programs which allow them to direct the malicious code to seek out sensitive information. The cable says that at least some of the attacks in 2008 originated from a Shanghai-based hacker group linked to the People’s Liberation Army’s Third Department, which oversees intelligence-gathering from electronic communications.

Between April and October 2008, hackers successfully stole "50 megabytes of email messages and attached documents, as well as a complete list of usernames and passwords from an unspecified (U.S. government) agency," the cable says.

Investigators say Byzantine Hades intrusions are part of a particularly virulent form of cyber-espionage known as an "advanced persistent threat." The malicious code embedded in attachments to spear-phish emails is often "polymorphic" - it changes form every time it runs - and burrows deep into computer networks to avoid discovery. Hackers also conduct "quality-assurance" tests in advance of launching attacks to minimize the number of anti-virus programs which can detect it, experts say.

As a result, cyber-security analysts say advanced persistent threats are often only identified after they penetrate computer networks and begin to send stolen data to the computer responsible for managing the attack. "You have to look for the ’phone home,’" says Roger Nebel, managing director for cyber-security at Defense Group Inc., a consulting firm in Washington, DC.

It was evidence of malicious code phoning home to a control server - a computer that supervises the actions of code inside other computers - that provided confirmation to U.S. cyber-sleuths that Chinese hackers were behind Byzantine Hades attacks, according to the April 2009 State Department cable.

As a case study, the cable cites a 10-month investigation by a group of computer experts at the University of Toronto which focused in part on cyber-intrusions aimed at Tibetan groups, including the office of the exiled Dalai Lama in Dharamsala, India.

Referencing the Canadian research, the cable notes that infected computers in the Dalai Lama’s office communicated with control servers previously used to attack Tibetan targets during the 2008 Olympics in Beijing. Two Web sites linked to the attack also communicated with the control server.

The same sites had also been involved in Byzantine Hades attacks on U.S. government computers in 2006, according to "sensitive reports" cited in the cable -- likely a euphemistic reference to secret intelligence reporting.

The computer-snooping code that the intrusion unleashed was known as the Gh0stNet Remote Access Tool (RAT). It "can capture keystrokes, take screen shots, install and change files, as well as record sound with a connected microphone and video with a connected webcam," according to the cable.

Gh0st RAT succeeded in invading at least one State Department computer. It "has been identified in incidents - believed to be the work of (Byzantine Hades) actors - affecting a locally employed staff member at the U.S. Embassy in Tokyo, Japan," according to the cable.

Evidence that data was being sucked out of a target network by malicious code also appears to have led cyber-security investigators to a specific hacker, affiliated with the Chinese government, who was conducting cyber-espionage in the United States. A March, 2009 cable identifies him as Yinan Peng. The cable says that Peng was believed to be the leader of a band of Chinese hackers who call themselves "Javaphile."

Peng did not respond to three emails seeking comment.

The details of alleged Chinese military-backed intrusions of U.S. government computers are discussed in a half dozen State Department cables recounting intense global concern about China’s aggressive use of cyber-espionage.

In a private meeting of U.S., German, French, British and Dutch officials held at Ramstein Air Base in September 2008, German officials said such computer attacks targeted every corner of the German market, including "the military, the economy, science and technology, commercial interests, and research and development," and increase "before major negotiations involving German and Chinese interests," according to a cable from that year.

French officials said at the meeting that they "believed Chinese actors had gained access to the computers of several high-level French officials, activating microphones and Web cameras for the purpose of eavesdropping," the cable said.

The leaked State Department cables have surfaced as Reuters has learned that the U.S. is engaged in quiet, proxy-led talks with China over cyber issues.

Chronic computer breaches have become a major source of tension in U.S. relations with China, which intensified after the major Google hack was disclosed in January 2010, according to U.S. officials involved in the talks. Even before the Google hack, Chinese officials had recognized the problem as well.

In mid-2009, representatives of the China Institutes for Contemporary International Relations, a nominally-independent research group affiliated with China’s Ministry of State Security, contacted James A. Lewis, a former U.S. diplomat now with the Center for Strategic and International Studies.

Lewis said that in his first meeting with his Chinese counterparts, a representative of the China Institutes asked: "Why does the Western press always blame China (for cyber-attacks)?" Lewis says he replied: "Because it’s true."

There was no response to request for comment on the talks from the Chinese embassy in Washington.

Preliminary meetings at CSIS have blossomed into three formal meetings in Washington and Beijing over the last 14 months. According to two participants, the talks continue to be marked by "a lot of suspicion." Attendees have focused on establishing a common understanding of cyber-related military, law enforcement and trade issues. Cyber-espionage isn’t being discussed directly, according to one participant, because "the Chinese go rigid" when the subject is raised.

One reason: for China, digital espionage is wrapped into larger concerns about how to keep China’s economy, the world’s second largest, growing. "They’ve identified innovation as crucial to future economic growth - but they’re not sure they can do it," says Lewis. "The easiest way to innovate is to plagiarize" by stealing U.S. intellectual property, he adds.

There have been a few breakthroughs. U.S. and Chinese government officials from law enforcement, intelligence, military and diplomatic agencies have attended in the wings of each discussion. "The goal has been to get both sides on the same page," says Lewis. "We're building the groundwork for official discussions."

A former senior national security official who has also attended the talks says, "Our reports go straight to the top policymakers" in the Obama administration.

Chinese participants have sought to allay U.S. concerns about a Chinese cyber-attack on the U.S. financial system. With China owning more than $1.1 trillion in U.S. government debt, Lewis says China's representatives acknowledged destabilization of U.S. markets would, in effect, be an attack on China's economy, itself.

Despite the talks, suspected Chinese cyber-espionage has hardly tapered off. Documents reviewed by Reuters show that CSIS itself recently was the target of a spear-phish containing malicious code with a suspected link to China.

On March 1, an email sent from an address on an unofficial U.S. Armed Forces family welfare network called AFGIMail was sent to Andrew Schwartz, chief spokesman for CSIS. Attached to the message was an Excel spreadsheet labeled "Titan Global Invitation List."

An analysis conducted for Reuters by a cyber-security expert who asked not to be identified shows the email may have been sent from a compromised AFGIMail email server. The Excel spreadsheet, if opened, installs malicious code which searches for documents on the victim's computer. The code then communicates to a Web-site hosting company in Orange County, California that has additional sites in China.

SpyEye Arrests Have Little Impact in the Grand Scheme

Reports are emerging from the UK that authorities have arrested three individuals in connection with the SpyEye botnet. Unfortunately, these appear to be bit players rather than the brains behind the SpyEye malware platform, and will have virtually no impact on the threat of SpyEye in general.

Arresting these guys is a bit like making a drug bust of the thug selling dime bags on the corner while the real drug kingpin sips piæa coladas in a villa on the beach in Costa Rica. The arrest might temporarily stop drugs from being sold on that particular block in that particular neighborhood, but have virtually no impact on drug trafficking as a whole. Another thug will be standing on that same corner selling the same dime bags tomorrow.

AppRiver, agrees with the drug dealer/drug lord analogy, but adds that even relatively trivial arrests such as these send a message that law enforcement is not going to tolerate such activity, and that it has the skills and capabilities to track down the attackers.

AppRiver's Troy Gill concurs with Touchette's opinion that the arrests send a message. He points out that the arrests still disrupt criminal activity on some level, and let other would-be script kiddies know that there is risk involved with cybercrime. Gill also notes that information gathered from these low-level players might contribute to the greater goal of tracking down the SpyEye source.

Vikram Thakur, principle security response manager for Symantec, commented, "Perhaps a more accurate analogy would be the arrest of someone who uses a gun to commit a crime, while the source that individual obtained the gun from remains free," adding "Regardless of the analogy, these individuals were caught stealing money from multiple banks. My assumption is that this involved a substantial monetary loss, since it warranted an investigation by law enforcement officials that appears to have lasted more than three months."

Thakur notes that individuals who are directly affected by botnets or malware attacks are primarily interested in simply catching the perpetrators of their particular crime. They aren’t necessarily concerned with the big picture of whether or not law enforcement manages to track down and prosecute the source of the tool that was used.

McAfee’s Dave Marcus has a more ominous take on the big picture, though. Marcus agrees that the individuals arrested are essentially script kiddies, but says that even if authorities arrested the authors of the SpyEye malware toolkit it would have little impact on the overall threat of SpyEye. Marcus notes "The code is out there, and will continue to be developed."

Is it good news that UK authorities put a stop to the criminal activity of these three individuals? Absolutely. But, ultimately it means little in the grand scheme of malware attacks.

Firefox Challenges Browser Rivals with Quicker Updates

Mozilla notified developers late last week that it intends to adopt a shorter development cycle for Firefox browser releases. Though this will help Firefox avoid losing more market share to Google’s Chrome - and put more pressure on Microsoft to follow suit with Internet Explorer - the real winner is the browser user, noted Net Applications Executive Vice President Vince Vizzaccaro.

"We’re seeing a commitment from all of the major browser providers to devote additional resources to their browsers, and to enhance and update them much more quickly than any time before in the history of the Internet," Vizzaccaro said. "They understand that browser users have options fostered by competition."

There are a lot of benefits to smoothing and streamlining development processes to release functionality on a more incremental basis, noted Al Hilwa, director of applications software development at IDC. "This is something Microsoft and other software developers have to grapple with," Hilwa said.

According to Net Applications, Internet Explorer’s share of the global browser market held steady in March at 55.92. Firefox (21.80 percent) was second, followed by Chrome (11.57 percent), Apple’s Safari (6.61 percent), and Opera (2.15 percent).

Since IE9 only had a 3.6 percent usage share in March, Microsoft’s new browser has had minimal impact on the browser market so far. One reason is that IE9 is not compatible with Windows XP, which "currently has 54 percent of global usage share," the web-metrics firm noted.

Over the long run, however, IE9 could potentially make big gains since it has been designed to take advantage of the rich graphics capabilities of Windows 7 and its underlying 64-bit hardware, Net Applications said.

"Windows 7 usage share is following a strong, fairly linear path upward," it observed. "And Windows versions from Vista forward should have a majority share within a couple of years."

Mozilla hopes to thwart Microsoft’s long-term strategy for IE9 by speeding up its browser release schedule. For example, it will stagger Firefox’s four stages of development - called the Mozilla-central, Mozilla-aurora, Firefox-beta and Mozilla-release channels - so that a general Firefox release can ship at week 16 and potentially as soon as every six weeks thereafter.

However, Firefox 5’s ship date will be slightly different from future releases due to the lack of a development overlap with Firefox 4. "Rather than six weeks for Mozilla-central, Mozilla-aurora, and Mozilla-beta, we instead have three weeks for development on Mozilla-central, five weeks to converge and stabilize on Mozilla-aurora, and five weeks to validate on Mozilla-beta," the browser maker noted.

The normal development schedule - under which every step in the cycle takes six weeks - will begin with Firefox 6’s development cycle, which "starts when Firefox 5 is cloned from Mozilla-central to Mozilla-aurora on April 12, Mozilla said. In other words, Firefox 6 potentially could ship before the end of summer.

Firefox’s market share has been slowly declining in recent months due to the rising popularity of the Chrome browser, which Google updates frequently and even on an automatic basis.

"Chrome’s development model has been a successful experiment in terms of getting production releases with improvements and new features out quickly and much faster than in the past," Hilwa said. "I think this is causing waves in the industry, most specifically for direct competitors."

While Firefox 4 sports a "check for updates" menu item and an update screen, an automatic browser update was postponed to Firefox 5. Additionally, support for 64-bit PC platforms is reportedly high on Mozilla’s list for Firefox 5.

"Firefox has certainly upped its game and is trying hard to fight the battle with Chrome for the power user where Chrome has gained share," Hilwa said.

Microsoft Unveils First Internet Explorer 10 Preview

Microsoft has released the first platform preview for Internet Explorer 10, less than a month after the launch its much-hyped Internet Explorer 9 browser.

The technology giant unveiled IE10 earlier today at its Mix11 developer conference in Las Vegas. The preview, which is now available for download, isn’t a reinvention of the browser (Microsoft’s goal with IE9), but rather a continuation of the work it did in hardware acceleration, HTML5 and CSS3.

"IE10 builds on full hardware acceleration and continues our focus on site-ready Web-standards," IE corporate vice president Dean Hachamovitch said in an announcement. "This combination enables developers to deliver the best performance for their customers on Windows while using the same, Web-standard markup across browsers."

Hachamovitch said that Microsoft is only three weeks into IE10’s development, but it’s already comfortable showing off what it has built so far. On stage at the Mix11 conference, he demonstrated some of its capabilities against Google’s Chrome browser and revealed that IE10 will include additional support for CSS3, including Gradients and the Flexible Box layout. Additional IE10 previews will be rolling out every eight to twelve weeks.

Microsoft released IE9 on March 14 after 40 million downloads during its beta. IE9 has been well received; at its peak, IE9 was downloaded 27 times per second. Still, Microsoft knew that it couldn’t rest on its laurels. Mozilla’s Firefox 4 browser was downloaded 5,000 times per minute during its first day of availability, and Google Chrome is already at version 11.

Apple Adds ’Do Not Track’ Option to Safari

Apple has jumped on the "do not track" bandwagon by adding the privacy tool to a test version of its Safari browser, according to the Wall Street Journal.

The "do not track" option is included in Lion, the next version of Apple’s Mac OS X. It’s currently only available to developers, and scheduled to be released later this year. The Journal said mentions of "do not track" started popping up in Web forums and on Twitter; Apple has not made any formal announcements.

A "do not track" option basically provides Web users with the option to not have their online activity tracked. This type of data is highly valuable to ad networks, which can use it to serve up more targeted advertisements. In many cases, relevant ads can be helpful to the Web surfer, but there is a concern that the average person has no idea what type of information is actually being collected. "Do not track" will provide them more control, according to supporters.

Google, Microsoft, and Mozilla already incorporate versions of "do not track" into their browsers.

The "Advanced" screen in Mozilla’s Firefox 4 Options tool now includes a box that, when checked, tells Web sites that you want to opt-out of tracking used for behavioral advertising. Mozilla added the feature to a pre-build version of Firefox in January, and added it to the beta in February.

Microsoft Tracking Protection was included in the release candidate of Internet Explorer 9, which was announced earlier this year. At the launch event for the RC, Microsoft also announced four partners for Tracking Protection: Abine, TRUSTe, PrivacyChoice, and AdBlock Plus. These firms will provide lists of sites that plant small tracking code on many other Web sites to profile users’ site history and habits. The Tracking Protection feature in IE9, which was first introduced in December, will allow users to block this snooping by either using one of these lists or automatically determining the offending Web domains. In later February, the World Wide Web Consortium (W3C), a Web standards body, gave Microsoft’s plan its stamp of approval.

Google, meanwhile, has a Chrome extension called Keep My Opt-Outs, which empowers users to permanently opt out of ad-tracking cookies.

"Do not track" initiatives got moving in December when the Federal Trade Commission unveiled a broad plan for online privacy, which included the "do not track" provision.

Congress has also stepped into the debate. In February, Rep. Jackie Speier introduced the Do Not Track Me Online Act of 2011, which would give the FTC 18 months to come up with standards for companies to follow when it comes to online tracking.

Just this week, Sens. John Kerry and John McCain also introduced a commercial "privacy bill of rights" that would give users more control over how their information is used on the Web, while Rep. Cliff Stearns, a Florida Republican, introduced a similar measure in the House, dubbed the Consumer Privacy Protection Act of 2011.

Dell 15-Inch Tablet-Laptop Combo Revealed

Thanks to leaked FCC schematics and specs, word is out that Dell is developing a new convertible tablet and notebook combo. The 15-inch device, code named the "Dell Panerai", may follow in the footsteps of the 10-inch Inspiron Duo convertible, though it’s not clear whether the Panerai will feature the same flip design.

What we do know from the FCC filing is that the Panerai will have both a "laptop mode" and a "tablet mode" and that there’s an Intel Centrino 6230 wireless chipset a/b/g/n.

That’s not a lot to go on, but while we wait for an official Dell announcement we can hope and dream that the Panerai will overcome the Duo’s shortcomings (namely, a short battery life and sluggish performance from its underpowered Atom processor). One of those new Intel Core i5 or i7 processors would be nice - and perhaps not unreasonable, considering the presence of the Intel Centrino 6 series card, typically paired with Sandy Bridge processors.

Asus Transformer, may offer the best of both worlds - if they can deliver on both the touch experience and mobile computing power. The Panerai’s 15-inch display size seems massive for a tablet, but roomy enough for traditional laptop work and entertainment.

One thing we can be sure of is that computer manufacturers are getting ever more inventive with tablet and laptop concepts.

Harvard Twins Stuck with Facebook Agreement

A federal appeals court ruled Monday that former Harvard University schoolmates of Facebook founder Mark Zuckerberg can’t undo their settlement over creation of the social networking site.

The 9th U.S. Circuit Court of Appeals said Monday that Tyler and Cameron Winklevoss were savvy enough to understand what they were agreeing to when they signed the agreement in 2008. The deal called for a $20 million cash payment and a partial ownership of Facebook. A third classmate, Divya Narendra, was part of the settlement with the twins but did not pursue the second lawsuit seeking to undo the agreement.

Monday’s ruling upholds a lower court decision enforcing the settlement during the six years of litigation that grew so contentious that the dispute was dramatized in the Oscar-nominated film, "The Social Network."

The settlement is now worth more than $160 million because of Facebook’s increased valuation.

The twins had alleged they were misled about Facebook’s value when they agreed to settle their lawsuit that claimed Zuckerberg stole their idea to launch Facebook.

"At some point, litigation must come to an end," chief justice Alex Kozinksi wrote for the unanimous three-judge panel "That point has now been reached."

The twins alleged they were misled into believing the company was worth $35.90 a share because of an investment by Microsoft Corp. But they argued that the company later valued the company at $8.88 for tax purposes. The twins argue they would have demanded more stock in the company based on the lower valuation.

Kozinski said the twins were "sophisticated parties" when they agreed to the settlement during a mediation meeting.

"They brought half-a-dozen lawyers to the mediation," Kozinksi wrote.

Facebook said Monday it was pleased by the ruling. Lawyers for the Winklevoss twins said they are reviewing the decision and have not decided on their next step. The twins could ask the Supreme Court to consider the case.

Allure of iPad, Other Tablets Hurting PC Sales

Last year, the popularity of Apple Inc.’s iPad hurt PC sales. This year, that trend is continuing, as new data from two market research firms indicate PC shipments declined in the first three months of 2011.

On Wednesday, Gartner Inc. said that its research shows PC shipments dipped 1.1 percent compared to the same period last year, to 84.3 million. IDC said its numbers show PC shipments fell 3.2 percent to 80.6 million. The companies measure the market in different ways.

Gartner had expected 3 percent shipment growth, while IDC was looking for 1.5 percent growth.

Gartner principal analyst Mikako Kitagawa said that during the January-March period consumers weren’t as drawn to cheap PCs - usually a category that keeps the market growing. Rather, they were interested in tablet computers and other consumer electronics.

"With the launch of the iPad 2 in February, more consumers either switched to buying an alternative device, or simply held back from buying PCs," Kitagawa said. "We’re investigating whether this trend is likely to have a long-term effect on the PC market."

For years, companies tried to popularize tablets, but it wasn’t until Apple released the iPad last April that the category took off. Last month, Apple started selling a new version of the device, and a bevy of companies including Hewlett-Packard Co., Dell Inc. and BlackBerry maker Research In Motion Ltd. are trying to catch up by offering their own takes on the tablet.

IDC attributes the PC shipment decline to several factors, including frugal businesses and a lack of consumer interest. To be successful over time, PC makers must find a better way to sell computers than simply touting their hardware specifications, IDC senior research analyst Jay Chou said.

"’Good-enough computing’ has become a firm reality, exemplified first by Mini Notebooks and now Media Tablets. Macroeconomic forces can explain some of the ebb and flow of the PC business, but the real question PC vendors have to think hard about is how to enable a compelling user experience that can justify spending on the added horsepower," he said.

In the U.S., IDC said shipments fell 10.7 percent to 16.1 million. Gartner has PC shipments falling 6.1 percent, also to 16.1 million.

Both firms have Palo Alto-based Hewlett-Packard Co. as the world’s top PC maker: Gartner said HP had nearly 18 percent of the market in the first quarter, while IDC pegs it at almost 19 percent.

But Gartner puts Taiwan’s Acer Inc. in the No. 2 spot, with almost 13 percent of the market and Round Rock, Texas-based Dell Inc. as No. 3, with nearly 12 percent. IDC, meanwhile, has Dell in the second-place spot, with almost 13 percent of the market, and Acer third, with slightly more than 11 percent.

Stateside, they both agree HP and Dell took the No. 1 and No. 2 spots, respectively, but Gartner’s data placed Acer and Japan-based Toshiba Corp. in third and fourth, while IDC’s data showed Toshiba in third and Apple, of Cupertino, in fourth.

=~=~=~=

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.